

T. Aruga #
Filed 3/19/01 2
Q63638
10f1

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日

Date of Application:

2000年 3月22日

出 願 番 号

Application Number:

特願2000-079917

出 願 人

Applicant(s):

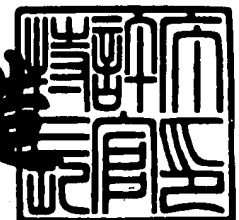
日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 2月 9日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3005105

11033 U.S. PRO
09/810220
03/19/01

【書類名】 特許願

【整理番号】 53209294PE

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00
G06F 12/14

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 有賀 俊裕

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100083987

【弁理士】

【氏名又は名称】 山内 梅雄

【手数料の表示】

【予納台帳番号】 016252

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9006535

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 携帯端末装置

【特許請求の範囲】

【請求項 1】 秘匿すべき情報を記憶する記憶手段と、

この記憶手段に記憶された前記情報の読み出しあるいは書き込みを行うための制御信号を生成する制御信号生成手段と、

この制御信号生成手段によって生成された前記制御信号および前記情報が伝送される 1 または複数の信号伝送路と、

少なくともこれら信号伝送路の 1 つに挿入され、前記記憶手段に記憶された前記情報にアクセスしないときのみこの信号伝送路を電氣的に遮断することによって前記情報へのアクセスを無効化する無効化手段とを具備することを特徴とする携帯端末装置。

【請求項 2】 秘匿すべき情報を記憶する記憶手段と、

この記憶手段に記憶された前記情報の読み出しあるいは書き込みを行うための制御信号を生成する制御信号生成手段と、

第 1 あるいは第 2 の状態のいずれかに切り替えるためのスイッチ手段と、

このスイッチ手段によって前記第 1 の状態に切り替えられている状態のとき前記制御信号を前記記憶手段に伝送し、前記第 2 の状態に切り替えられている状態のとき不正アクセスとして前記制御信号を無効化する無効化手段とを具備することを特徴とする携帯端末装置。

【請求項 3】 前記記憶手段はパスワードを受け付けこれがあらかじめ登録されたパスワードと一致したときのみ前記情報のアクセスを承認する着脱自在の記憶媒体であることを特徴とする請求項 1 または請求項 2 記載の携帯端末装置。

【請求項 4】 前記記憶手段が貨幣価値を電子的に置き換えた電子マネーを記憶する着脱自在の電子マネーカードであって、前記スイッチ手段によって前記第 1 の状態に切り替えられたとき所定の時間単位で引き出される電子マネーの金額を測定する測定手段と、この測定手段によって測定された前記電子マネーの金額があらかじめ決められた金額を超えたか否かを判別する判別手段と、この判別手段によって前記あらかじめ決められた金額を超えたと判別されたとき前記電子

マネーカードへのアクセスを拒否する処理中止手段とを備えることを特徴とする請求項 2 または請求項 3 記載の携帯端末装置。

【請求項 5】 ネットワークからデータを受信する無線通信手段を備えることを特徴とする請求項 1 ～請求項 4 記載の携帯端末装置。

【請求項 6】 ネットワークからデータを受信する無線通信手段と、装置本体の正面に配置され前記無線通信手段によって受信された前記データに基づいて文字、画像等を表示する表示手段とを備え、前記スイッチ手段は前記装置本体側面に配置されていることを特徴とする請求項 2 ～請求項 4 記載の携帯端末装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は携帯端末装置に係わり、例えば秘匿すべき個人情報をアクセスする携帯端末装置に関する。

【 0 0 0 2 】

【従来の技術】

近年の集積化技術、実装化技術あるいは通信技術等の進歩にともない、携帯電話機に代表される通信機能を有する携帯端末装置から、コンピュータネットワークが相互に接続されたインターネット上の各種サーバにアクセスできるようになった。これにより、携帯端末装置は、その表示部を用いて、電子メールの送受信のみならず、各種サーバから取得したコンテンツデータによる文字や画像等の情報を表示させることができる。このような携帯端末装置によるコンテンツデータの取得を行うシステムとして、例えばワイヤレスアプリケーションプロトコル（Wireless Application Protocol：以下、WAP と略す。）システムがある。

【 0 0 0 3 】

WAP システムにおける携帯端末装置によりインターネット上の各種サーバにアクセスしてオンラインショッピングや決済等によって金銭の授受が行われる場合のようにネットワークを介して携帯端末装置等から決済等を行う場合、個人認証が必要とされる。この個人認証は、従来携帯端末装置のテンキーボードから利用者にパスワードを入力させていたが、利用者の操作性を向上するため端末装置

に装着されたＩＣカードに記憶された個人情報を利用することが可能となっている。一般的にＩＣカードには、個人認証に必要なパスワードがあらかじめ登録されており、ＩＣカードはアクセスを要求されたとき、パスワードを受け付け、この登録されたパスワードと一致するときのみ、そのアクセス要求を受け入れる。このようなＩＣカードとして、例えば貨幣価値を電子的に置き換えた電子マネーを管理する電子マネーカードがある。

【0004】

このように外部であるネットワーク上の各種サーバから種々のコンテンツデータを取得する携帯端末装置では、秘匿すべき個人情報にアクセスするための電子マネーカードのようなＩＣカードが装着される場合もあり、その記憶情報の漏洩についての安全性には万全を期す必要がある。例えば携帯端末装置が第三者に渡った場合、盗み見等によってその個人のパスワードを知っていたことになると個人情報への不正アクセスや不正決済等をもはや防止することができなくなる。そこで、このような携帯端末装置の安全性を向上させる技術について、種々提案されている。

【0005】

例えば特開平9-223112号公報「正規利用者認識装置および使用方法」に開示された携帯端末装置は、複数個のスイッチを備え、あらかじめこれらのスイッチ状態の組み合わせを登録しておく。そして、これらスイッチの押下状態が一致したときにのみ、携帯端末装置のテンキーボードを介して入力されたパスワードの照合処理を行う。これにより、パスワードの盗み見が行われた場合であっても、スイッチの押下状態の組み合わせを盗み見される可能性がほとんどないため、安全性の高い携帯端末装置を提供することができる。

【0006】

また例えば特開平11-30953号公報「電子財布・電子マネー連携セキュリティシステム」に開示された携帯端末装置は、あらかじめ指定した金額分だけ電子マネーを利用することで支払い時の過大抜き取りを防止する。

【0007】

さらにまた例えば特開平11-96262号公報「マルチメディア携帯端末を

用いた電子マネー取引方式」には、網膜パターンと指紋とを各個人の認証情報として組み合わせることによって安全性を向上させた携帯端末装置に関する技術が開示されている。

【 0 0 0 8 】

【発明が解決しようとする課題】

しかしながら W A P システムに適用されるような携帯端末装置は、外部であるインターネット上の各種サーバから表示部に表示させるための表示情報や、場合によっては装置内で実行する制御プログラムをコンテンツデータとして取得するような場合、ウイルスや不正のプログラムが携帯端末装置内に侵入してしまう危険性がある。従来提案された携帯端末装置では、その個人認証をソフトウェア処理によって行うため、侵入したウイルスや不正のプログラムによって、秘匿すべき個人情報を記憶する電子マネーカード等の I C カードに不正にアクセスしてデータを読み出したり、破壊するといった可能性がある。あるいは、例えば第三者が内密に通信機能を使って不正に端末にアクセスし、同様の不正行為が行われる可能性もある。または、その可能性があることに対する携帯端末装置の利用者の心理的負担がある。

【 0 0 0 9 】

したがってこのような不正行為が行われないように、携帯端末装置の安全性を考慮した設計を行う必要がある。しかし従来提案された携帯端末装置に関する技術では、網膜や指紋による複雑な認証処理は処理負荷がかかり、複数のスイッチを備えることは装置の大型化を招く。これは、できるだけ端末の負荷を軽減させる W A P システムに適用されるような携帯端末装置にとっては不都合となる。

【 0 0 1 0 】

そこで本発明の目的は、第三者による不正行為があった場合であっても安全性を保ち、その個人認証処理にともなう負荷を削減することができる携帯端末装置を提供することにある。

【 0 0 1 1 】

【課題を解決するための手段】

請求項 1 記載の発明では、（イ）秘匿すべき情報を記憶する記憶手段と、（ロ

）この記憶手段に記憶された前記情報の読み出しあるいは書き込みを行うための制御信号を生成する制御信号生成手段と、（ハ）この制御信号生成手段によって生成された前記制御信号および前記情報が伝送される１または複数の信号伝送路と、（ニ）少なくともこれら信号伝送路の１つに挿入され、前記記憶手段に記憶された前記情報にアクセスしないときのみこの信号伝送路を電氣的に遮断することによって前記情報へのアクセスを無効化する無効化手段とを携帯端末装置に具備させる。

【 0 0 1 2 】

すなわち請求項１記載の発明では、秘匿すべき情報を記憶する記憶手段を備える携帯端末装置に、この秘匿すべき情報の読み出しあるいは書き込みを行うための制御信号を生成する制御信号生成手段を設け、制御信号生成手段と記憶手段との間にこれら制御信号が伝送される１または複数の信号伝送路を備えた。そして、少なくともこれら信号伝送路の１つに無効化手段を挿入し、記憶手段に記憶された情報にアクセスしないときのみこの信号伝送路を電氣的に遮断することによって情報へのアクセスを無効化するようにした。

【 0 0 1 3 】

請求項２記載の発明では、（イ）秘匿すべき情報を記憶する記憶手段と、（ロ）この記憶手段に記憶された前記情報の読み出しあるいは書き込みを行うための制御信号を生成する制御信号生成手段と、（ハ）第１あるいは第２の状態のいずれかに切り替えるためのスイッチ手段と、（ニ）このスイッチ手段によって前記第１の状態に切り替えられている状態のとき前記制御信号を前記記憶手段に伝送し、前記第２の状態に切り替えられている状態のとき不正アクセスとして前記制御信号を無効化する無効化手段とを携帯端末装置に具備させる。

【 0 0 1 4 】

すなわち請求項２記載の発明では、秘匿すべき情報を記憶する記憶手段と、これにアクセスするための制御信号を生成する制御信号生成手段とを備える携帯端末装置に、第１および第２の状態のいずれかに切り替えることができるスイッチ手段を設けるようにした。そして、スイッチ手段によって第１の状態に切り替えられている状態のとき制御信号生成手段によって生成された制御信号を記憶手段

に伝送して秘匿すべき情報にアクセスできるようにし、第2の状態に切り替えられている状態のとき制御信号を無効化して、秘匿すべき情報にアクセスできないようにした。

【 0 0 1 5 】

請求項3記載の発明では、請求項1または請求項2記載の携帯端末装置で、前記憶手段はパスワードを受け付けこれがあらかじめ登録されたパスワードと一致したときのみ前記情報のアクセスを承認する着脱自在の記憶媒体であることを特徴としている。

【 0 0 1 6 】

すなわち請求項3記載の発明では、記憶手段として、パスワードを受け付けこれがあらかじめ登録されたパスワードと一致したときのみ記憶情報のアクセスを承認するICカードや電子マネーカード、加入者情報を記憶する記憶モジュールといった着脱自在の記憶媒体とした。

【 0 0 1 7 】

請求項4記載の発明では、請求項2または請求項3記載の携帯端末装置で、記憶手段が貨幣価値を電子的に置き換えた電子マネーを記憶する着脱自在の電子マネーカードであって、スイッチ手段によって第1の状態に切り替えられたとき所定の時間単位で引き出される電子マネーの金額を測定する測定手段と、この測定手段によって測定された電子マネーの金額があらかじめ決められた金額を超えたか否かを判別する判別手段と、この判別手段によってあらかじめ決められた金額を超えたと判別されたとき電子マネーカードへのアクセスを拒否する処理中止手段とを備えることを特徴としている。

【 0 0 1 8 】

すなわち請求項4記載の発明では、電子マネーカードが装着される携帯端末装置について、測定手段によりスイッチ手段によって第1の状態に切り替えられたとき所定の時間単位で引き出される電子マネーの金額を測定し、判別手段によりこの測定した金額があらかじめ決められた金額を超えたか否かを判別させる。そして、この判別手段によってあらかじめ決められた金額を超えたと判別されたとき電子マネーカードへのアクセスを拒否するようにした。

【 0 0 1 9 】

請求項 5 記載の発明では、請求項 1 ～請求項 4 記載の携帯端末装置で、ネットワークからデータを受信する無線通信手段を備えることを特徴としている。

【 0 0 2 0 】

すなわち請求項 5 記載の発明では、無線通信手段を備えた携帯端末装置に適用するようにした。

【 0 0 2 1 】

請求項 6 記載の発明では、請求項 2 ～請求項 4 記載の携帯端末装置で、ネットワークからデータを受信する無線通信手段と、装置本体の正面に配置され無線通信手段によって受信されたデータに基づいて文字、画像等を表示する表示手段とを備え、スイッチ手段は装置本体側面に配置されていることを特徴としている。

【 0 0 2 2 】

すなわち請求項 6 記載の発明では、例えば片手の指で携帯端末装置本体を保持しながらスイッチ手段を押下しやすいように、本体の側面に配置するようにした。

【 0 0 2 3 】

【発明の実施の形態】

【 0 0 2 4 】

【実施例】

以下実施例につき本発明を詳細に説明する。

【 0 0 2 5 】

図 1 は、本発明の一実施例における携帯端末装置が適用される情報通信システムの構成の概要を表わしたものである。本実施例における携帯端末装置 1 0 は、ネットワーク 1 1 を介してコンテンツサーバ 1 2 と接続されている。携帯端末装置 1 0 は、例えば液晶ディスプレイ（Liquid Crystal Display：以下、LCD と略す。）からなる表示部を備え、ネットワーク 1 1 を介して受信したデータをこの表示部に表示できるようになっている。さらにこの携帯端末装置 1 0 は、電子マネーカードのような秘匿すべき個人情報を記憶する着脱自在の IC カードがあらかじめ決められた装着部に装着され、正規利用者によってその記憶情報を自在

に読み出しおよび書き込みができるようになっているものとする。ネットワーク 11 は、例えば携帯電話網であり、携帯端末装置 10 はその通信形態に応じて、コンテンツサーバ 12 との間でデータの送受信を行う。コンテンツサーバ 12 には、文字、画像等の各種データ形式の情報からなるコンテンツデータが格納されている。

【0026】

このような情報通信システムでは、携帯端末装置 10 がネットワーク 11 を介してコンテンツサーバ 12 にアクセスする。そして、このコンテンツサーバ 12 に格納されているコンテンツデータを受信して一時的に記憶し、その表示部に表示させる。受信したコンテンツデータがオンラインショッピングのようなホームページで、携帯端末装置 10 に電子マネーカードが装着されている場合、携帯端末装置 10 の利用者は、例えばその表示内容にしたがって端末装置のテンキーボードを介して購入するものを指定した後、装着される電子マネーカードから電子マネーを引き出すための個人認証のためのパスワードを指定する。指定したパスワードが照合されると装着される電子マネーカードから電子マネーが引き出され、購入するものを特定する購入情報に続いて送信される。携帯端末装置 10 によって送信された購入情報と電子マネーは、ネットワーク 11 を介して、コンテンツサーバ 12 で受信される。コンテンツサーバ 12 に上述したコンテンツデータを格納させた管理者は、携帯端末装置 10 の利用者が契約する決済業者に対しこの受信した電子マネーの決済を行う。

【0027】

本実施例における携帯端末装置 10 は、セキュリティボタンを備え、端末装置の利用者がこのセキュリティボタンを押下することによって端末装置に装着される電子マネーカードをアクセスするための制御信号を強制的に遮断することができるようになっている。以下、このような携帯端末装置 10 について説明する。

【0028】

図 2 は、本実施例における携帯端末装置の構成の概要を表わしたものである。携帯端末装置 10 は、図示しない装着部に装着され秘匿すべき個人情報を記憶する着脱自在の IC カード 20 と、図 1 に示したネットワーク 11 を介して各種デ

ータを送受信するための通信機能およびＩＣカード２０に記憶された個人情報に対するアクセス機能を有するシステム部２１と、端末装置１０の利用者によって押下されるセキュリティボタン２２とを備えている。ＩＣカード２０には、個人認証に必要なパスワードがあらかじめ登録されており、外部からＩＣカード２０内の記憶情報の読み出しあるいは書き込みが要求されたとき、この登録されたパスワードを受け付け、これと一致するときのみ要求を受け入れる。システム部２１は、そのアクセス機能によりＩＣカード２０をアクセスするためのＩＣカード制御信号を生成する。このＩＣカード制御信号は、装着されるＩＣカード２０とシステム部２１との間のインタフェース仕様によって異なり、例えば読出制御信号、書込制御信号、データバス信号があるが、これらに限定されるものではない。

【 0 0 2 9 】

システム部２１によって生成されたＩＣカード制御信号は、ＩＣカード制御信号線２３を介しＩＣカード２０に対して電氣的に伝送される。ＩＣカード２０に記憶された個人情報は、このＩＣカード制御信号に応じて書き込みあるいは読み出しが行われ、読み出し時にはＩＣカード制御信号線２３を介し個人情報等が電氣的にシステム部２１に対して送信される。このようにＩＣカード２０とシステム部２１とをハードウェア的に接続するＩＣカード制御信号線２３のうち少なくとも１つは、ゲート回路２４が挿入されている。

【 0 0 3 0 】

ゲート回路２４は、セキュリティボタン２２の押下状態に応じて、回路内のスイッチを開閉するようになっている。このスイッチの開閉によって、ゲート回路２４を挿入されたＩＣカード制御信号線の電氣的な接続状態、あるいは遮断状態に切り替える。すなわち、携帯端末装置１０のセキュリティボタン２２が利用者によって物理的に押下されている状態のとき、ゲート回路２４のスイッチが閉状態となってＩＣカード制御信号線が電氣的に接続状態となりシステム部２１からのＩＣカード制御信号によるＩＣカード２０へのアクセスが可能となる。これに対して、携帯端末装置１０の利用者がセキュリティボタン２２を離すと、ゲート回路２４のスイッチが開状態となって、ＩＣカード制御信号線が電氣的に遮断状

態となり、システム部 2 1 からの I C カード制御信号による I C カード 2 0 へのアクセスが不可能となる。

【 0 0 3 1 】

これにより、携帯端末装置 1 0 の利用者がセキュリティボタン 2 2 を押下した状態ではない限り、システム部 2 1 は I C カード 2 0 にアクセスすることができず、第三者が利用者に無断でネットワークを介して携帯端末装置 1 0 に侵入し、システム部 2 1 にアクセスして I C カード 2 0 の記憶情報の破壊や読み出しを防止することができる。

【 0 0 3 2 】

次にこのような本実施例における携帯端末装置として携帯電話機を例に具体的に説明する。

【 0 0 3 3 】

図 3 は、本実施例における携帯端末装置としての携帯電話機の外観を正面から表わしたものである。本実施例における携帯端末装置としての携帯電話機 3 0 は、本体の正面に L C D からなる表示部 3 1 と、表示部 3 1 と同一面上に配置されたテンキーボード 3 2 と、本体側面に配置されたセキュリティボタン 3 3 と、本体の上側の側面に設けられたアンテナ 3 4 とを備えている。さらにこの携帯電話機 3 0 は、本体の裏面あるいは内部に着脱自在の電子マネーカードを装着するための装着部が設けられており、ここではこの装着部に電子マネーカード 3 5 が装着されているものとする。

【 0 0 3 4 】

図 4 は、図 3 で示した携帯端末装置としての携帯電話機の構成要部を表わしたものである。ただし、図 3 に示す携帯電話機と同一部分には同一符号を付している。本実施例における携帯端末装置としての携帯電話機は、携帯電話システム部 4 0 を備え、これにアンテナ 3 4、表示部 3 1 およびテンキーボード 3 2 が接続されている。携帯電話システム部 4 0 は、テンキーボード 3 2 から入力された利用者の指示にしたがってアンテナ 3 4 から送信する無線電波によりネットワーク上のコンテンツサーバと通信接続し、受信したコンテンツの内容を表示部 3 1 に表示させる。また、携帯電話システム部 4 0 は、電子マネーカード 3 5 にアクセ

スするための電子マネーカード制御信号を生成する。電子マネーカード制御信号は、電子マネーカード制御信号線 4 1 を介してゲート回路 4 2 に入力される。ゲート回路 4 2 は、セキュリティボタン 3 3 の押下状態に応じて電子マネーカード制御信号線 4 1 を電氣的に接続状態あるいは遮断状態に切り替える。接続状態となったとき、電子マネーカード制御信号線 4 3 を介して携帯電話システム部 4 0 によって生成された電子マネーカード制御信号を電子マネーカード 3 5 に伝送する。

【 0 0 3 5 】

ゲート回路 4 2 は、コントロール端子付きバッファ 4 4 と、コントロール信号発生回路 4 5 とを備えている。コントロール端子付きバッファ 4 4 の入力端子には、電子マネーカード制御信号線 4 1 が接続され、その出力端子には電子マネーカード制御信号線 4 3 が接続される。コントロール端子付きバッファ 4 4 は、コントロール端子から入力されるコントロール信号が電氣的レベルが所定の“H”レベルを超えていることを示すハイボルト状態のとき、その出力端子をハイインピーダンス状態とする。一方、コントロール信号の電氣的レベルが所定の“L”レベルを超えていないことを示すローボルト状態のとき、その出力端子からは入力端子から入力された電子マネーカード制御信号を電氣的に増幅して電子マネーカード 3 5 に対して出力する。コントロール信号発生回路 4 5 は、コントロール端子付きバッファ 4 4 のコントロール端子に入力するコントロール信号を生成する。

【 0 0 3 6 】

コントロール信号発生回路 4 5 は、セキュリティボタン 3 3 の押下状態に応じて開閉状態が切り替えられるスイッチ 4 6 を備え、このスイッチ 4 6 のチャタリングを防止するチャタリング防止回路から構成されているものとする。スイッチ 4 6 の一方は接地され、他方は第 1 の抵抗素子 4 7 を介してコントロール端子付きバッファ 4 4 のコントロール端子に接続される。第 1 の抵抗素子 4 7 とスイッチ 4 6 の接続点は、コンデンサ 4 8 を介して接地されるるとともに、第 2 の抵抗素子 4 9 を介して電源電圧レベルに接続される。

【 0 0 3 7 】

このような構成のコントロール信号発生回路 4 5 は、セキュリティボタン 3 3 が押下されていないとき、スイッチ 4 6 は開状態となり、コントロール端子に供給されるコントロール端子は第 1 および第 2 の抵抗素子 4 7、4 9 を介して電源電圧レベルに接続され、電氣的にハイボルト状態となる。したがって、コントロール端子付きバッファ 4 4 は、その出力端子をハイインピーダンス状態とするため、電子マネーカード制御信号線 4 1、4 3 は電氣的に遮断状態となって、携帯電話システム部 4 0 で生成された電子マネーカード制御信号は電子マネーカード 3 5 に伝達されない。

【 0 0 3 8 】

一方、携帯電話機の利用者によってセキュリティボタン 3 3 が押下されているとき、スイッチ 4 6 は閉状態となり、コントロール端子に供給されるコントロール端子は第 1 の抵抗素子 4 7 を介して接地され、電氣的にローボルト状態となる。したがって、コントロール端子付きバッファ 4 4 は、入力端子に接続された電子マネーカード制御信号線 4 1 を伝達される電子マネーカード制御信号を電氣的に増幅し、電子マネーカード制御信号線 4 3 に接続された出力端子から電子マネーカード 3 5 に対して出力する。すなわち、電子マネーカード制御信号線 4 1、4 3 は電氣的に接続状態となって、携帯電話システム部 4 0 で生成された電子マネーカード制御信号は電子マネーカード 3 5 に伝達される。

【 0 0 3 9 】

これにより図 4 に示した携帯電話機は、セキュリティボタン 3 3 を押下していない状態では携帯電話システム部 4 0 は電子マネーカード 3 5 にアクセスすることができず、セキュリティボタン 3 3 を押下している状態では携帯電話システム部 4 0 は電子マネーカード 3 5 にアクセスすることができる。

【 0 0 4 0 】

続いて、このようなゲート回路 4 2 を介して電子マネーカード 3 5 と接続され、電子マネーカード 3 5 に対しアクセスするための電子マネーカード制御信号を生成する携帯電話システム部 4 0 の動作について説明する。この携帯電話システム部 4 0 は、図示しない中央処理装置 (Central Processing Unit: CPU) を有し、読み出し専用メモリ (Read Only Memory: ROM) 等の所定の記憶装置に

格納された制御プログラムにしたがって電子マネーカードに対するアクセス処理を実行することができるようになっている。

【 0 0 4 1 】

図 5 は、電子マネーカードにアクセスする携帯電話システム部の処理内容の概要を表わしたものである。図 3 に示す携帯電話機の利用者が、テンキーボード 3 2 を介してネットワーク 1 1 上のコンテンツサーバ 1 2 に格納されたコンテンツデータの取得を指定すると、携帯電話機はネットワーク 1 1 を介してコンテンツサーバ 1 2 にアクセスして指定されたコンテンツデータの取得要求を行う。取得要求されたコンテンツデータはアンテナ 3 4 を介して受信され、表示部 3 1 に表示される。

【 0 0 4 2 】

携帯電話システム部 4 0 は、電子マネーの使用イベントの発生の有無を監視する（ステップ S 5 0 : N）。ここで、受信したコンテンツデータが、通信販売の案内であって端末装置の利用者が電子マネーによる支払いを行う場合、電子マネーの使用イベントが発生する。携帯電話システム部 4 0 はこのイベントの発生を検出すると（ステップ S 5 0 : Y）、表示部 3 1 に電子マネー使用要求の表示を行う（ステップ S 5 1）。

【 0 0 4 3 】

この表示部 3 1 に表示された電子マネー使用要求表示としては、例えば携帯電話機の利用者に電子マネー使用イベントを承認するときセキュリティボタン 3 3 を押下させ、承認しないときセキュリティボタン 3 3 を押下させないように指示する旨を表示させる。

【 0 0 4 4 】

携帯電話システム部 4 0 は、セキュリティボタン 3 3 の押下状態にかかわらず、電子マネー使用イベントを継続し、テンキーボード 3 2 からの電子マネーの使用に必要な情報の入力を受け付ける（ステップ S 5 2）。携帯電話システム部 4 0 は、この受け付けた入力情報にしたがって電子マネーカード 3 5 に対する電子マネーカード制御信号を生成するとともに、電子マネーカード制御信号線を介して電子マネーカード 3 5 に対して送出する（ステップ S 5 3）。

【 0 0 4 5 】

ステップ S 5 3 で電子マネーカード制御信号を出力すると、所定のタイムアウト時間の計時を開始し、電子マネーカード 3 5 からの応答があるか否かを監視する（ステップ S 5 4）。所定の応答タイムアウト時間を経過するまでにステップ S 5 3 で出力した電子マネーカード制御信号に対応する電子マネーカード 3 5 から応答があったとき（ステップ S 5 4 : N）、所定の電子マネー使用処理を実行し（ステップ S 5 5）、電子マネー使用処理完了ではない限り（ステップ S 5 6 : N）、ステップ S 5 3 に戻ってテンキーボード 3 2 からの電子マネーの使用に必要な情報の入力を受け付ける。

【 0 0 4 6 】

ステップ S 5 6 で、電子マネー使用処理が完了したとき（ステップ S 5 6 : Y）、電子マネー使用完了メッセージを表示部 3 1 に表示し（ステップ S 5 7）、再び電子マネー使用イベントの発生を監視する（リターン）。

【 0 0 4 7 】

ステップ S 5 4 において、所定の応答タイムアウト時間を経過してステップ S 5 3 で出力した電子マネーカード制御信号に対応する電子マネーカード 3 5 からの応答がなかったとき（ステップ S 5 4 : Y）、セキュリティボタン 3 3 が押下されていない状態であって、携帯電話機の利用者が電子マネー使用イベントを承認していないものと判断し、表示部 3 1 に電子マネー使用不可メッセージを表示し（ステップ S 5 8）、所定の電子マネー使用中止処理を行って電子マネーの使用処理を中止する。その後、再び電子マネー使用イベントの発生を監視する（リターン）。

【 0 0 4 8 】

このように本実施例における携帯端末装置は、セキュリティボタンの押下状態にかかわらず電子マネーの使用処理を実行し、所定のタイムアウト時間の経過によりセキュリティボタンの押下状態を検出することで、ウイルスや不正プログラムによる不正行為によってセキュリティボタンの押下状態の検出をも誤らせないようにしている。

【 0 0 4 9 】

なお、このような携帯端末装置については、図4に示したコントロール端子付きバッファ44に代えて種々の代替手段が考えられる。

【0050】

図6は、図4に示したコントロール端子付きバッファと同様の機能を果たす論理回路の構成を表わしたものである。すなわち、コントロール信号発生回路45で生成されたコントロール信号60が入力される否定回路61と、一方が否定回路61の出力端子に接続され他方が携帯電話システム部40によって生成された電子マネーカード制御信号62が入力される2入力1出力AND回路63とからなる。このような論理回路では、コントロール信号60を論理反転し、電子マネーカード制御信号62と論理積を演算し、その結果を電子マネーカード制御信号64として電子マネーカード35に対して送出する。これにより、セキュリティボタン33が押下されていない状態では、常に論理レベル“L”の電子マネーカード制御信号64を出力させることができる。なお、コントロール信号発生回路の構成によって、スイッチ46の開状態でコントロール信号がローボルト、スイッチ46の開状態でコントロール信号がハイボルトとなる場合には、否定回路61を省略する。

【0051】

また、図4では、携帯電話システム部40によって生成された電子マネーカード制御信号が電子マネーカード35に対して送出されるものとして説明したが、これに限定されるものではない。その逆として、電子マネーカード制御信号が電子マネーカードから出力され携帯電話システム部に供給される場合にはコントロール端子付きバッファのバッファ方向を逆にすればよい。また、電子マネーカード制御信号が携帯電話システム部と電子マネーカードとの間で双方向で伝送される場合、コントロール端子付きバッファに代えて、コントロール付きトランシーバを用いればよい。

【0052】

さらにまた、電子マネーカード制御信号線41、43は1本のみを示しているが、これに限定されるものではない。電子マネーカード制御信号線が複数本の場合には、そのうちの1本あるいは所定の数だけゲート回路を挿入するようにすれ

ばよい。

【 0 0 5 3 】

以上説明したように本実施例における携帯端末装置としての携帯電話機は、秘匿すべき個人情報等を記憶する着脱自在のＩＣカードとしての電子マネーカードと、これにアクセスするための電子マネーカード制御信号を生成する携帯電話機システム部４０と、セキュリティボタン３３とを備え、セキュリティボタン３３が押下されているときのみ、携帯電話機システム部４０から電子マネーカード３５にアクセスするために電子マネーカード制御信号が伝送される電子マネーカード制御信号線が電氣的に接続されるようにした。

【 0 0 5 4 】

これにより、セキュリティボタン３３が押下されていない状態では、電子マネーカード３５にはアクセスすることができないので、例えば第三者がネットワーク１１を介してアンテナから携帯電話システム部４０に侵入し、電子マネーカードに不正アクセス、あるいは電子マネーの窃盗、電子マネーカード内の記憶情報の破壊といった行為を防止することができる。また、第三者がアンテナを通して携帯電話システム部４０内部に電子マネーカードを不正アクセスするためのウィルスのような不正プログラムを常駐させ、利用者がセキュリティボタンを押下したときに不正プログラムが電子マネーカードにアクセスした場合であっても、利用者はセキュリティボタンの押下前後の電子マネーカード内の情報を検査することによって不正プログラムの侵入とその損害を不正アクセス直後に検出することができる。したがって、不正アクセスへの対処も迅速に行うことができ、万が一不正アクセスが行われた場合であってもその損害額を少なくすることができる。

【 0 0 5 5 】

変形例

【 0 0 5 6 】

本実施例における携帯端末装置としての携帯電話機では、アンテナを通して不正プログラムが常駐していた場合、図５に示したようにセキュリティボタンが押下されている限り、その不正アクセスが行われてしまう可能性がある。そこで、本変形例における携帯端末としての携帯電話機では、所定の時間内における電子

マネーカードから引き出される金額に制限を設けて、常駐している不正プログラムにより多額の電子マネーが窃盗されることを防止する。

【 0 0 5 7 】

本変形例における携帯電話機の構成は、図 3 および図 4 に示したように本実施例における携帯電話機と同様であるため説明を省略する。

【 0 0 5 8 】

図 7 は、本変形例における電子マネーカードにアクセスする携帯電話システム部の処理内容の概要を表わしたものである。ただし、図 5 に示した本実施例における携帯電話システムの処理内容と同一部分には同一符号を付し、説明を省略する。本変形例における携帯電話機の動作が、図 5 に示した本実施例における携帯電話機の動作と異なるところは、ステップ S 7 0 ～ステップ S 7 2 が挿入された点である。

【 0 0 5 9 】

すなわち、ステップ S 5 4 で、所定の応答タイムアウト時間を経過するまでに電子マネーカード 3 5 から応答があったとき（ステップ S 5 4 : N）、取扱い金額データの測定を開始し（ステップ S 7 0）、所定の電子マネー使用処理を実行する（ステップ S 5 5）。この取扱い金額データは、所定の計測時間単位に計測される電子マネーカードから引き出される電子マネーの金額である。

【 0 0 6 0 】

使用処理実行（ステップ S 5 5）後は、この取扱い金額データの測定を終了し（ステップ S 7 1）、電子マネーカードから引き出される電子マネーの金額が、あらかじめ決められた金額内にあるか否かを判別する（ステップ S 7 2）。あらかじめ決められた金額内にあると判別されたとき（ステップ S 7 2 : Y）、ステップ S 5 6 で使用処理が完了したか否かを判定する（ステップ S 5 6）。一方、ステップ S 7 2 で、測定した取扱い金額データがあらかじめ決められた金額内ないと判別されたとき（ステップ S 7 2 : N）、不正プログラムによる窃盗の可能性が高いと判断し、表示部 3 1 に電子マネー使用不可メッセージを表示し（ステップ S 5 8）、所定の電子マネー使用中止処理を行って電子マネー使用処理を中止する。その後、再び電子マネー使用イベントの発生を監視する（リターン）

【 0 0 6 1 】

このように本変形例における携帯端末装置としての携帯電話機では、本実施例における携帯電話機に対して所定の計測時間単位に電子マネーカードから引き出せる金額の制限を設けたので、これを超える電子マネーの引き出しを不正プログラムによる窃盗の可能性が高いと判断することによって、セキュリティボタンが押下されている状態で常駐している不正プログラムにより多額の電子マネーが窃盗されることを防止することができる。

【 0 0 6 2 】

なお本実施例および本変形例における携帯端末装置としての携帯電話機により、電子マネーを引き出すとき、セキュリティボタンを押下状態で、電子マネーのパスワードを入力するためのテンキーボードの操作を容易にするため、セキュリティボタンの配置位置を工夫することも可能である。例えば、片手の指でテンキーボードを操作しもう一方の手で携帯電話機を保持しながらセキュリティボタンを押下しやすいように、セキュリティボタンを本体の左側面、あるいは右の側面に配置する。また、携帯電話機を、鞆等に入れた状態で、不用意にセキュリティボタンを押下状態として、第三者に不正アクセスされないように、セキュリティボタンを携帯電話機に窪みを付けて隠れるようにしたり、セキュリティボタンを複数設けて同時に押されたときのみ電子マネーカードにアクセスできるようにしたり、あるいはセキュリティボタンにカバーを付ける構造を採用することも可能である。

【 0 0 6 3 】

なおさらに本変形例における携帯端末装置としての携帯電話機については、コントロール信号をコントロール端子付きバッファのみならず携帯電話システム部の割り込み入力信号と兼用にすることによって、携帯電話システム部が電子マネーカードから電子マネーを引き出すことを利用者が許可したかどうかを容易に知ることができ、万が一不正アクセスが行われても引き出される電子マネーの金額に制限が設けられているためその損害を最小限にして、不正アクセスの有無の現状を知ることができる。

【 0 0 6 4 】

なおさらにまた本実施例および本変形例における携帯端末装置では、電子マネーカードについて説明したが、これに限定されるものではないことは当然である。その他の秘匿すべき個人情報を記憶することができるＩＣカードでもよい。さらに、携帯端末装置としての携帯電話機に加入者ごとに装着される加入者情報モジュールのようにあらかじめ記憶される加入者情報のうち、その一部あるいは全部について、セキュリティボタンが押下されたときのみ加入者情報へのアクセスを行うようにすることも可能である。

【 0 0 6 5 】

【発明の効果】

以上説明したように請求項１記載の発明によれば、物理的に秘匿すべき情報に対するアクセスを遮断することができるようにしたので、携帯端末の利用者の意図に反する第三者によるウイルスや不正プログラムによる情報のアクセスを容易かつ確実に防止することができる。また、その個人認証にともなう複雑な処理を新たに付加する必要がなくなり、装置の小型化および低コスト化に貢献することができる。

【 0 0 6 6 】

また請求項２記載の発明によれば、スイッチ手段によって所定の状態に切り替えられない限り、記憶手段に記憶された秘匿すべき情報へのアクセスを行うことができないようにしたので、携帯端末装置の利用者の意図に反する第三者のソフトウェアによるアクセスを効果的に防止することができる。また、第三者による不正アクセスが行われた場合であっても、スイッチ手段の切替前後の記憶手段に記憶された情報を検査することによって不正行為とその損害を行為の直後に検出することができ、不正行為への対処も迅速に行うことができる。このため、万が一不正行為が行われた場合であってもその損害を最小限にすることができる。

【 0 0 6 7 】

さらに請求項３記載の発明によれば、ＩＣカードや電子マネーカード、加入者情報を記憶する記憶モジュールといった着脱自在の記憶媒体を装着するようにしたので、個人認証の便宜の向上にともなう不正行為に対する安全性を維持するこ

とができる。

【0068】

さらにまた請求項4記載の発明によれば、所定の計測時間単位に電子マネーカードから引き出せる金額の制限を設けたので、これを超える電子マネーの引き出しを不正プログラムによる窃盗の可能性が高いと判断することによって、セキュリティボタンが押下されている状態で常駐している不正プログラムにより多額の電子マネーが窃盗されることを防止することができる。

【0069】

さらに請求項5記載の発明によれば、無線通信手段を備えた携帯端末装置に適用するようにしたので、ネットワークの外部からのデータ受信とともにウイルスが侵入したり、例えば第三者がネットワークを介して侵入し、秘匿すべき情報を記憶する記憶手段に不正なアクセス、あるいは情報の窃盗、記憶情報を破壊するといった行為による危険性を大幅に低減することができる。

【0070】

さらにまた請求項6記載の発明によれば、例えば片手の指で携帯端末装置本体を保持しながらスイッチ手段を押下しやすいように、本体の側面に配置することによって、表示画面を参照しながら必要なときのみスイッチ手段を押下することができ、結果的に無駄にスイッチ手段が押下される時間を削減してその分不正行為の危険性を低減させることができる。

【図面の簡単な説明】

【図1】

本実施例における携帯端末装置が適用される情報通信システムの構成の概要を示す構成図である。

【図2】

本実施例における携帯端末装置の構成の概要を示すブロック図である。

【図3】

本実施例における携帯端末装置としての携帯電話機の外観を正面から表わす外観図である。

【図4】

本実施例における携帯端末装置としての携帯電話機の構成要部を示すブロック図である。

【図 5】

本実施例における電子マネーカードにアクセスする携帯電話システム部の処理内容の概要を示す流れ図である。

【図 6】

本実施例におけるコントロール端子付きバッファと同様の機能を果たす論理回路の構成を示す説明図である。

【図 7】

本変形例における電子マネーカードにアクセスする携帯電話システム部の処理内容の概要を示す流れ図である。

【符号の説明】

- 1 0 携帯端末装置
- 1 1 ネットワーク
- 1 2 コンテンツサーバ
- 2 0 ICカード
- 2 1 システム部
- 2 2、3 3 セキュリティボタン
- 2 3 ICカード制御信号線
- 2 4、4 2 ゲート回路
- 3 0 携帯電話機
- 3 1 表示部
- 3 2 テンキーボード
- 3 4 アンテナ
- 3 5 電子マネーカード
- 4 0 携帯電話システム部
- 4 1、4 3 電子マネーカード制御信号線
- 4 4 コントロール端子付きバッファ
- 4 5 コントロール信号発生回路

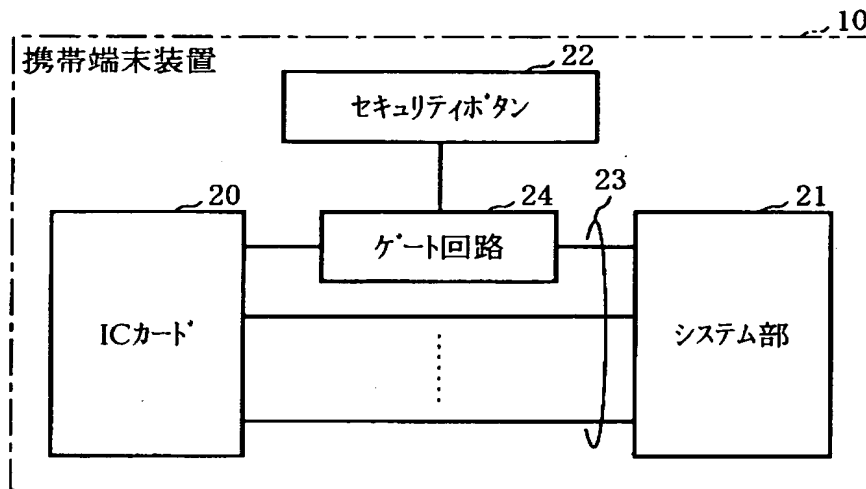
- 4 6 スイッチ
- 4 7 第 1 の抵抗素子
- 4 8 コンデンサ
- 4 9 第 2 の抵抗素子

【書類名】 図面

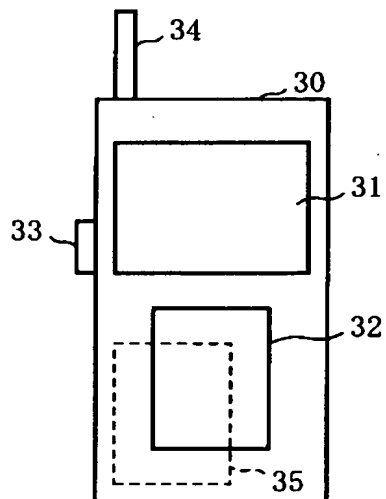
【図 1】



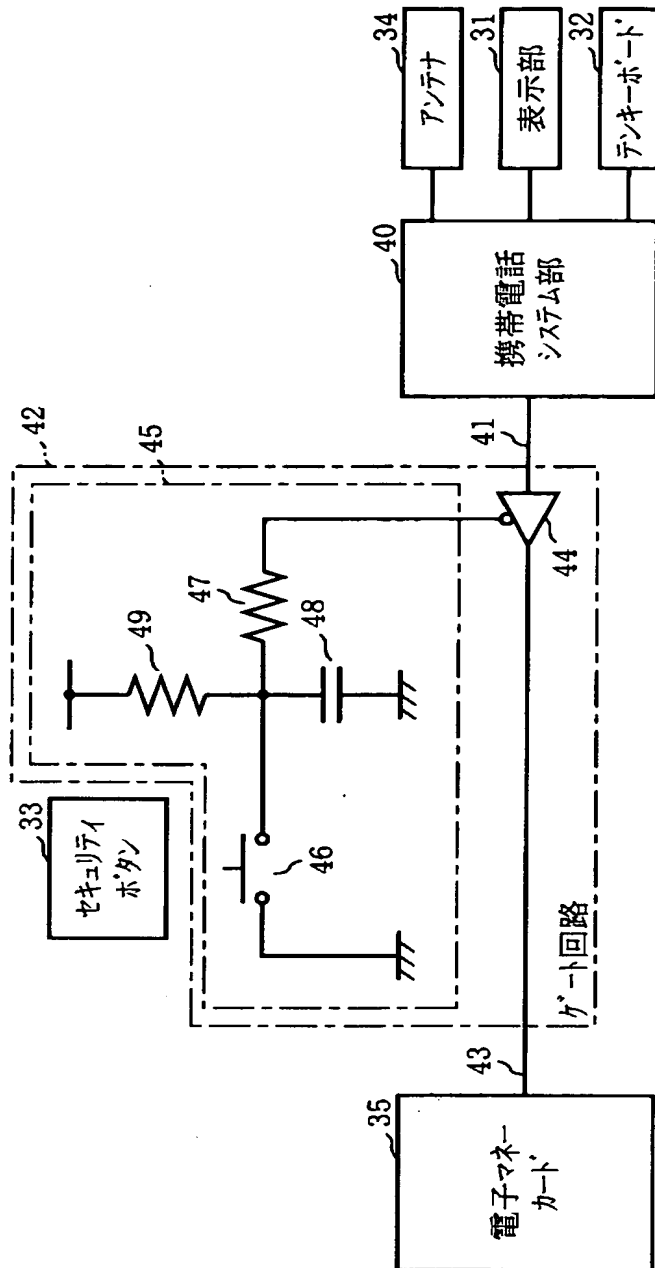
【図 2】



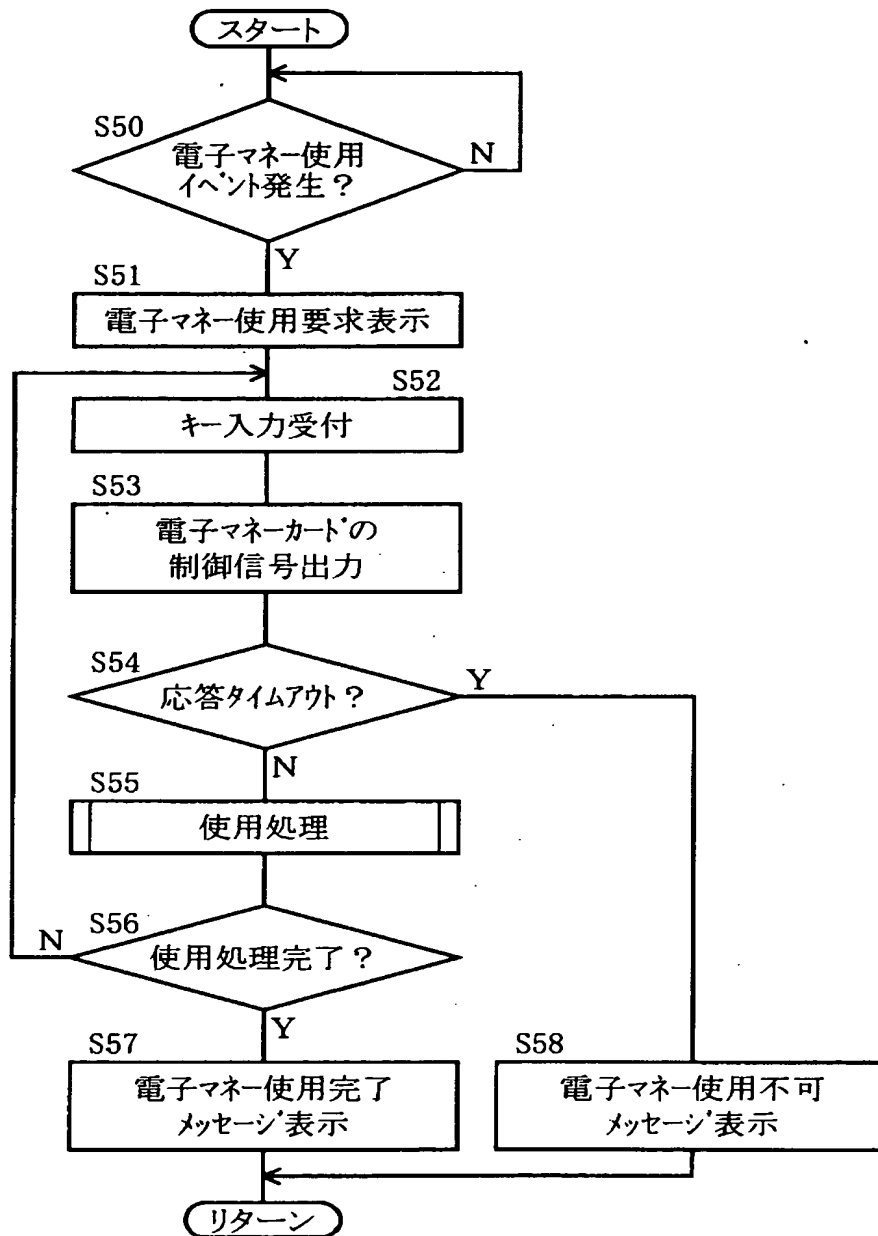
【図 3】



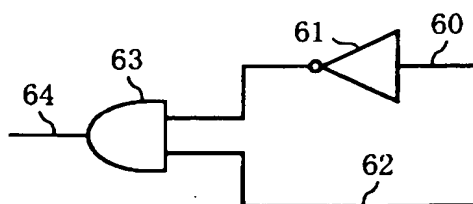
【図 4】



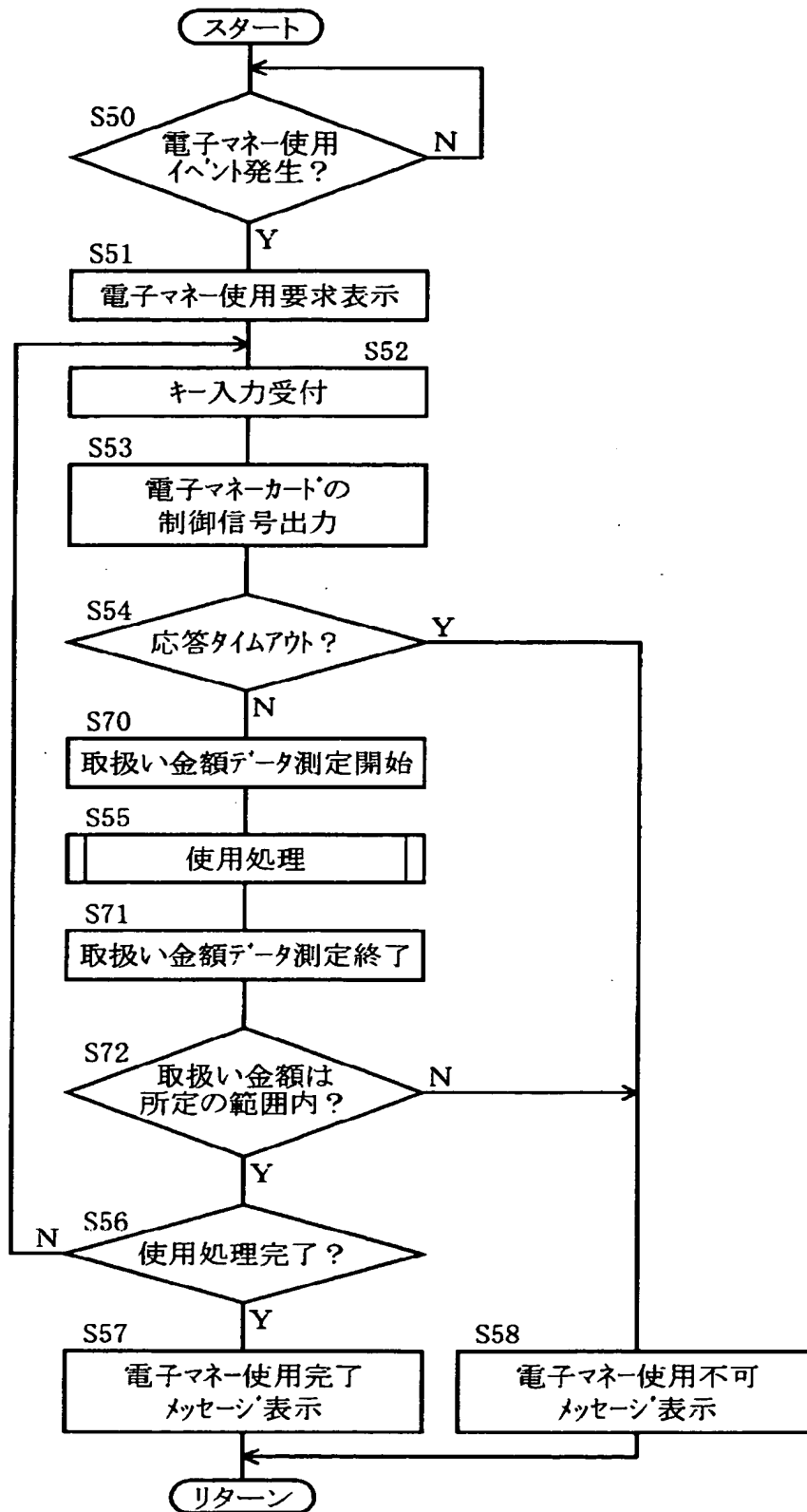
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 第三者による不正行為があった場合であっても安全性を保ち、その個人認証処理にともなう負荷を削減する携帯端末装置を提供する。

【解決手段】 秘匿すべき個人情報等を記憶する着脱自在のＩＣカード２０と、これにアクセスするためのＩＣカード制御信号を生成するシステム部２１と、セキュリティボタン２２とを備え、ゲート回路２４により、セキュリティボタン２２が押下されているときのみ、システム部２１からＩＣカード２０にアクセスするためにＩＣカード制御信号が伝送されるＩＣカード制御信号線が電氣的に接続される。

【選択図】 図２

認定・付加情報

特許出願の番号	特願2000-079917
受付番号	50000348114
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 3月23日

<認定情報・付加情報>

【提出日】	平成12年 3月22日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日
[変更理由] 新規登録
住 所 東京都港区芝五丁目7番1号
氏 名 日本電気株式会社